EXHIBIT 4

ISS'S STATEMENT OF ISSUES OF FACT THAT REMAIN TO BE LITIGATED

ISS reserves the right to modify, supplement, or change this Statement of Issues of Fact That Remain to be Litigated (the "Statement") to reflect the Court's rulings on any pending dispositive motions. ISS also reserves the right to modify, supplement or change this Statement to the extent necessary to fairly respond to any new issues SRI raises in its Statement of Issues of Fact. To the extent that any of these issues is deemed an issue of law rather than an issue of fact, ISS incorporates said issue by reference into ISS's Statement of Issues of Law that Remain to be Litigated. Conversely, to the extent that any issue in ISS's Statement of Issues of Law that Remain to be Litigated is deemed an issue of fact, ISS incorporates said issue by reference into this Statement.

This Statement of Issues of Fact applies only to the liability phase of trial. Issues of damages and willfulness have been bifurcated by the Court and will be addressed separately.

SRI has asserted the following claims against ISS (referred to herein as the "asserted ISS claims"):

Asserted ISS claims	• '338 patent: claims 1, 4, 5, 11, 12, 13, and 24 • '203 patent: claims 1, 2, 4, 6, 12, 13, 15, and 17 • '615 patent: claims 1, 2, 4, 13, 14, and 16

I. INFRINGEMENT

1. Whether, by a preponderance of the evidence, SRI can prove that the operation of RealSecure agents (Network, Guard, Server, and Desktop series) and Proventia agents (A, G, M, Server and Desktop series) (the "ISS sensors") when used in combination with the SiteProtector SecurityFusion Module 2.0 (as well as later versions) meets each and every limitation of the

asserted ISS claims of the ‘203 or ‘615 patents, either literally or with only insubstantial differences.

2. Whether, by a preponderance of the evidence, SRI can prove that ISS has directly infringed the asserted ISS claims of the ‘203 or ‘615 patents in the manner alleged to be infringing.

3. Whether, by a preponderance of the evidence, SRI can prove that any ISS customer has directly infringed the asserted ISS claims of the ‘203 or ‘615 patents in the manner alleged to be infringing.

4. Whether, by a preponderance of the evidence, SRI can prove that ISS, with the requisite intent and knowledge, actively induced its customers to operate one or more of the ISS sensors used in combination with the SiteProtector Security Fusion Module 2.0 (as well as later versions) to infringe the asserted ISS claims of the ‘203 and ‘615 patents.[1]

5. Whether, by a preponderance of the evidence, SRI can prove Proventia Network Anomaly Detection System (ADS) operating in standalone mode meets each and every limitation of the asserted ISS claims of the ‘338 patent, either literally or with only insubstantial differences.

6. Whether, by a preponderance of the evidence, SRI can prove that ISS has directly infringed the asserted ISS claims of the ‘338 patent in the manner alleged to be infringing.

7. Whether, by a preponderance of the evidence, SRI can prove that any ISS customer has directly infringed the asserted ISS claims of the ‘338 patent in the manner alleged to be infringing.

8. Whether, by a preponderance of the evidence, SRI can prove that ISS, with the requisite intent and knowledge, actively induced its customers to use the Proventia Network Anomaly Detection System (ADS) operating in standalone mode to infringe the asserted ISS claims of the ‘338 patent.

[1] ISS understands that SRI is no longer asserting contributory infringement against any ISS product.

II. INVALIDITY

9. Whether, for each claim, SRI can prove a date of invention earlier than the respective filing date, and such date of invention.

A. Anticipation

10. Whether the following printed publications are prior art under 35 U.S.C. § 102(a), (b), and (e):

- P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," ("*Live Traffic*" various versions);
- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20th National Information Systems Security Conference, pp. 353-365, October 9, 1997 ("*Emerald 1997*");[2]
- D. Anderson, T. Frivold, and A. Valdes, "Next-generation Intrusion Detection Expert System (NIDES) A Summary," Computer Science Laboratory, SRI-CSL-95-07, May 1995 ("*Network NIDES*");
- Y. Frank Jou et al., "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, April 1997 ("*JiNao Report*");
- L. Todd Heberlein et al., "A Network Security Monitor," Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296-304, May 1990 ("*NSM 1990*");
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, pp. 262-271, October 1992 ("*ISM 1992*");
- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol. 8 No. 3, pp. 26-41, June 1994 ("*NID 1994*");
- Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and a Proposed Distributed IDS Architecture," CSE-91-7, Feb. 1991 ("*DIDS Feb. 1991*");
- Steven R. Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype," Proc. 14th National Computer Security Conference, pp. 167-173, October 1991 ("*DIDS Oct. 1991*");

[2] The Court previously determined that EMERALD 1997 is a prior art printed publication under 102(b).

- S. Staniford-Chen et al., "GrIDS – A Graph Based Intrusion Detection System for Large Networks," 19th National Information Systems Security Conference, pp. 361-370, October 1996 ("*GrIDS 1996*");
- Steven Cheung et al., "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical Report, UC Davis Department of Computer Science, Davis California, May 14, 1997 ("*GrIDS 1997*");
- "NetStalker, Installation and User's Guide, Version 1.0.2" (May 1996);
- "RealSecure Release 1.0 for Windows NT 4.0 A User's Guide and Reference Manual"; and
- "NetRanger User's Guide Version 1.3.1," WheelGroup Corporation, 1997 ("*NetRanger Manual*").[3]

11. Whether the following systems or products were known or used before the inventions claimed, or were in public use or on sale prior to November 9, 1997:

- Network Security Monitor ("NSM");
- Distributed Intrusion Detection System ("DIDS");
- Graph-based Intrusion Detection System ("GrIDS");
- NetRanger;
- ISS RealSecure; and
- NetStalker.

12. Whether, by clear and convincing evidence,[4] ISS can prove that the above-listed printed publications, patents, systems or products satisfy each and every limitation of the asserted ISS claims of the '338, '203, and '615 patents, either explicitly or inherently.

B. Obviousness

The following references constitute "obviousness references" herein:

- All references listed in (10) above;
- All systems listed in (11) above;

[3] SRI has stipulated this is a 102(b) prior art reference.

[4] As discussed in Exhibit 6, section 1(A), Defendants request that the Court either (1) instruct the jury that Defendants need only prove invalidity by a preponderance of the evidence with respect to those issues on which PTO has initially rejected the claims during reexamination, or (2) instruct the jury that it may consider the PTO's decision to declare re-examinations and initially reject the claims-in-suit when determining whether or not Defendants have rebutted the presumption of validity and proven invalidity by clear and convincing evidence.

- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "A Method to Detect Intrusive Activity in a Networked Environment," Proc. 14th National Computer Security Conference, pp. 362-371, Oct. 1991;
- H.S. Javitz and A. Valdes, "The NIDES Statistical Component Description and Justification," Annual Report A010, March 1994;
- A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection using NIDES," Proc. of the Third International Workshop on Rough Sets and Soft Computing, January 1995;
- SunScreen EFS Configuration and Management Guide, Release 1.1, Rev. A, Sun Microsystems, June 1997;
- CERT Advisory CA-1996-21 TCP Syn Flooding and IP Spoofing Attacks;
- CERT Advisory CA-1996-26 "Denial-of-Service Attack via Ping, Dec. 18, 1996; and
- Any additional obviousness references relied upon in the Defendants' expert reports, including but not limited to additional references regarding the Network Security Monitor, the Distributed Intrusion Detection System, the Graph Based Intrusion Detection System, the ISS RealSecure system, the NetStalker system, and the NetRanger system.

13. Whether certain obviousness references are prior art under 35 U.S.C. § 102 (a), (b) or (e).

14. The level of ordinary skill in the art at the time of the invention of the '338, '203, and '615 patents.

15. Whether, by clear and convincing evidence, ISS can prove that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine certain obviousness references resulting in satisfaction of the limitations of the asserted ISS claims of the '338, '203, and '615 patents.

16. Whether, by clear and convincing evidence, ISS can prove that it would have been

obvious to one of ordinary skill in the art at the time of the invention to modify certain obviousness references resulting in satisfaction of the limitations of the asserted ISS claims of the ‘338, ‘203, and‘615 patents.

17. Whether there is any objective evidence of nonobviousness for any asserted patent claim, and whether SRI can prove a connection or nexus between any such objective evidence and the inventions of the asserted ISS claims.

18. Whether there is any objective evidence of obviousness for any asserted patent claim.

C. Best Mode

19. Whether, by clear and convincing evidence, ISS can prove that the common patent specification fails to disclose the best mode of practicing the asserted ISS claims of the ‘338, ‘203, and ‘615 patents.

D. Written Description

20. Whether, by clear and convincing evidence, ISS can prove that the common patent specification fails to describe to one of ordinary skill at the time of the invention each and every limitation of the asserted ISS claims of the ‘203 and ‘615 patents.

III. UNENFORCEABILITY

21. Whether individuals associated with the filing or prosecution of the ‘338, ‘203, and ‘615 patents either withheld information from the United States Patent & Trademark Office (the “PTO”) or misrepresented information to the PTO, including the following as disclosed in ISS’s Response to SRI’s Interrogatory No. 11, including all supplements thereto:

- Debra Anderson, Thane Frivold, and Alfonso Valdes, “Next-Generation Intrusion Detection Expert Systems (NIDES): A Summary,” SRI-CSL-95-07, May 1995;
- L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood, D. Wolber, “A Network Security Monitor,” Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, May 1990;
- Y. Frank Jou et al., Architecture Design of a Scalable Intrusion Detection System for

the Emerging Network, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997;

- Additional prior art references disclosed in ISS's Response to SRI's Interrogatory No. 11, including all supplements thereto; and
- Inequitable conduct with regard to the filing of the Appendix to the '203, '615, and '338 patents.

22. Whether, by clear and convincing evidence, ISS can prove that the withheld or misrepresented information was material.

23. Whether, by clear and convincing evidence, ISS can prove that the information was withheld or misrepresented with the intent to mislead or deceive the PTO.